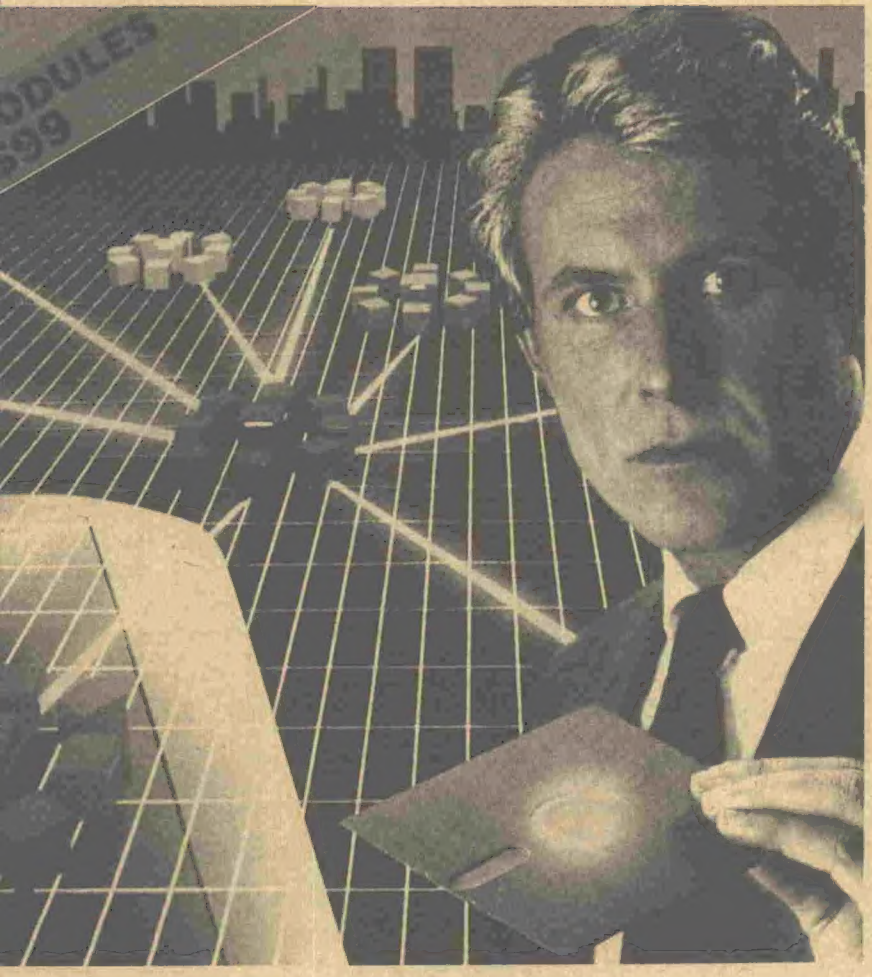
DATA SECURITY

สหัส พรหมสิทธิ์

LAN กับระบบการรักษาความปลอดภัยข้อมูล

ความเป็นมาของระบบการรักษาความปลอดภัยข้อมูลในแลนและมาตรการต่าง ๆ ที่นำมาใช้ พร้อมทั้งการยกตัวอย่างผลิตภัณฑ์ในระบบรักษาความปลอดภัยข้อมูล



การรักษาความปลอดภัย (security) เป็นเรื่องของการพิทักษ์ให้ความปลอดภัยแก่สิ่งที่มีค่า อันไม่เลือกว่าจะเป็นคอมพิวเตอร์หรือเป็นเน็ตเวอร์กของคอมพิวเตอร์ เช่น ระบบแลน (LAN) ซึ่งต่างก็มีความสำคัญในแง่ของการเป็นแหล่งเก็บสะสมตัวเลขข้อมูล และทรัพยากรเครื่องใช้ที่จะให้ใครมากระทำการอันมิชอบไม่ได้ ด้วยเหตุนี้จึงกำหนดให้มีมาตรการต่าง ๆ ที่จะมารักษาความปลอดภัยให้กับระบบคอมพิวเตอร์ดังกล่าว ในบทความนี้จะกล่าวเฉพาะเจาะจงไปที่ระบบคอมพิวเตอร์เน็ตเวอร์กซึ่งเรียกว่าระบบ "แลน" ด้วยกำลังได้รับความนิยมนำมาใช้กันแพร่หลายในธุรกิจอุตสาหกรรมต่าง ๆ อย่างมากในปัจจุบัน โดยจะขอเริ่มด้วยจุดแรกที่ว่า จะมีมาตรการอย่างไรที่จะมาทำให้แลนปลอดภัยจากการแทรกแซงจู่โจมอันมิชอบ

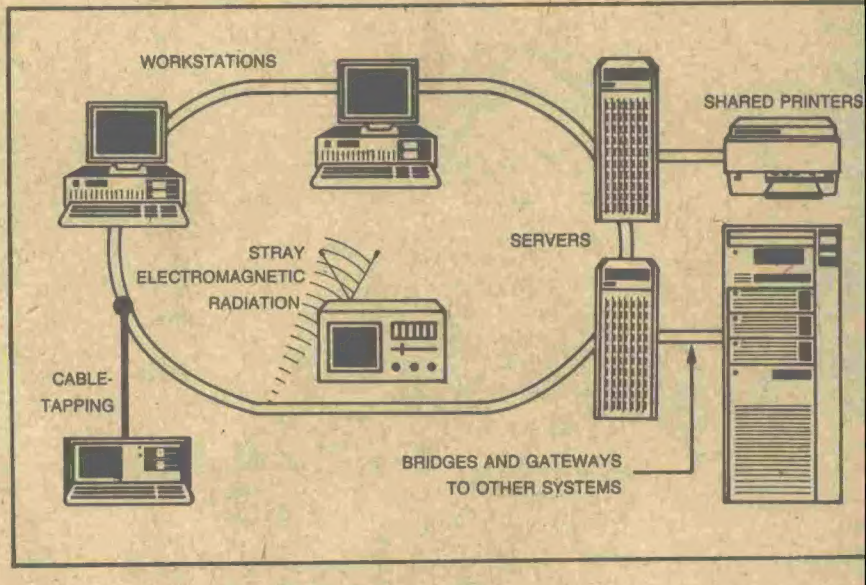
มาตรการความปลอดภัยในแลน

มาตรการในการรักษาความปลอดภัยสำหรับแลนซึ่งจะกล่าวในที่นี้ส่วนใหญ่จะมีที่มาจากประเทศสหรัฐอเมริกา อันได้กำหนดขึ้นมาโดยที่ทั้งภาครัฐ (เช่นกระทรวงกลาโหม) และภาคเอกชนเป็นผู้ร่วมกันทำด้วยการหยิบยืมแนวความคิดที่ดีที่สุดของแต่ละฝ่ายมาใช้ โดยได้มุ่งไปที่ประเด็นสำคัญ ๆ ดังนี้คือ

เอ็นคริปชัน (Encryption)

เอ็นคริปชัน เป็นกระบวนการในการกระจายข้อมูล (scramblingdata) เพื่อกลบเกลื่อนร่องรอยเดิมจนไม่มีอะไรเหลืออยู่ ก่อนที่จะส่งข้อมูลดังกล่าวเข้าไปในระบบเน็ตเวอร์ก เหตุที่ทำเช่นนี้ก็เพราะไม่ต้องการให้ผู้ที่ไม่เกี่ยวข้องสามารถล่วงรู้สิ่งที่มีอยู่ในข้อมูลนั้น ประกอบกับว่าการทำงานของแลนโดยทั่ว ๆ ไปยังมีจุดอ่อนที่ว่า ข้อมูลที่ส่งไปในจุดต่าง ๆ ในเน็ตเวอร์กเป็นการส่งแบบกระจายเสียงที่เป็นไปในรูปแบบที่โจ่งแจ้งชนิดไม่มีการปิดบังแต่อย่างใด อันทำให้สามารถแอบฟังได้ โดยเฉพาะในยุคที่เริ่มมีการใช้เครื่องมือการวิเคราะห์ระบบเน็ตเวอร์กกันอย่างแพร่หลายในปัจจุบัน ซึ่งจะทำให้การลักลอบแอบฟังเป็นไปอย่างสะดวกขึ้น เพราะเครื่องมือเหล่านี้ได้ออกแบบขึ้นมาให้เหมาะสำหรับติดตามดูความเป็นไปของระบบเส้นทางการสื่อสารในแลน (LAN Traffic) หรือความคับคั่งของสัญญาณต่าง ๆ ภายในแลนได้อย่างละเอียด อันทำให้จำเป็นต้องหาวิธีการบางอย่างมาทำให้ข้อมูลที่ส่งไปในเน็ตเวอร์กเป็นความลับ หนึ่งในวิธีการเช่นนี้ก็คือดาต้าเอ็นคริปชัน ดังได้อธิบายในข้างต้น คำว่า "เอ็นคริปชัน" นี้จะหมายถึงการคำนวณอย่างหนึ่งที่จะแปลงข้อมูลที่ใคร ๆ ก็รู้ได้ให้ไปอยู่ในอีกสภาพอีกอย่างหนึ่ง ในรูปแบบของรหัสที่ซับซ้อนจนคนส่วนใหญ่ไม่สามารถแปลงรหัสดังกล่าวให้กลับไปเป็นข้อมูลเหมือนในตอนแรกเริ่มได้ หรือถึงจะแปลงรหัสดังกล่าวได้ก็จะไม่คุ้มกับที่ต้องลงทุนลงแรงไปแต่อย่างใด เว้นแต่ว่าสิ่งที่อยู่ในรหัสนั้นจะมีสำคัญหรือมีสิ่งจูงใจมากจนคุ้มค่าที่ใครสักคนจะลงทุนทำทุกวิถีทางเพื่อแกะหรือถอดรหัสนั้น ๆ ให้กลับออกมาเป็นข้อมูลอันหาค่ามิได้ เช่นการล้วงความลับในระดับประเทศต่อประเทศ เมื่อเป็นเช่นนี้จึงสามารถกล่าวได้ว่า ดาต้าเอ็นคริปชันเป็นรากฐานของระบบการรักษาความปลอดภัยข้อมูลในระบบสื่อสารโทรคมนาคมที่ควรให้ความสำคัญเป็นอันดับแรก ดังนั้นก่อนที่จะกล่าวถึงเรื่องอื่นต่อไปก็จะขอวกกลับมาที่จุดแรก ๆ ที่เกี่ยวกับเรื่องของความเสี่ยงทางกายภาพในระบบแลนนั้นควรให้การระมัดระวังตรงส่วนใดบ้าง

จุดต่าง ๆ ที่ถือว่าล่อแหลมต่อความปลอดภัยของข้อมูลภายในแลนนั้นได้แสดงไว้แล้วในรูปที่ 1 โดยได้แสดงภยันตรายในลำดับแรกว่า มักจะอยู่ที่ตัวเซอร์ฟเวอร์ เวอร์กสเตชันและสายเคเบิ้ล ที่ต้องให้การเอาใจใส่เป็นพิเศษ เพราะจะอาศัยแค่เพียงการรักษาความปลอดภัยข้อมูลในรูปของซอฟต์แวร์และฮาร์ดแวร์มาช่วยเพียงอย่างเดียวไม่ได้ เช่นในกรณีเซอร์ฟเวอร์ที่ใช้งานดอสอยู่และมีไฟล์ต่าง ๆ ที่เก็บข้อมูลอยู่เป็นแบบดอสฟอร์แมตนั้นไม่สู้จะไม่ปลอดภัยนัก เพราะผู้บุกรุกเพื่อลักลอบดูข้อมูลอาจทำได้โดยสะดวกด้วยการเข้าไปดูไฟล์ต่าง ๆ โดยไม่ต้องอาศัยซอฟต์แวร์ของไฟล์เซอร์ฟเวอร์แต่อย่างใด เพียงแค่การบูตด้วยดอสเท่านั้นก็พอแล้ว วิธีป้องกันเรื่องนี้ทำได้หลายวิธี ยกตัวอย่างเช่น การเก็บตัวเซอร์ฟเวอร์ไว้ในบริเวณที่มีการควบคุมทางเข้าออกหรือการใช้เซอร์ฟเวอร์พาสส์เวิร์ดที่ยอมให้มีการบูตเครื่องได้แต่ไม่ยอมให้ใช้คีย์บอร์ดจนกว่าจะมี

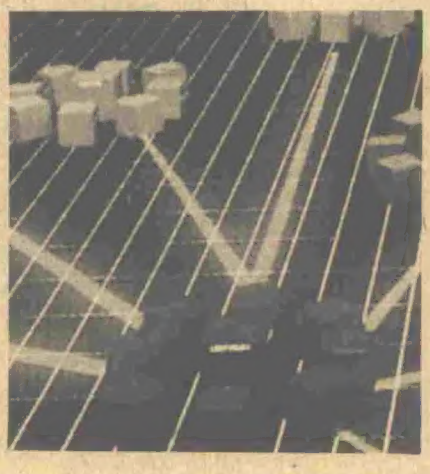


รูปที่ 1 ความล่อแหลมของในระบบเน็ตเวอร์ก เช่น กรณีของแลน นี้จะเกิดจากการกระจัดกระจายของอุปกรณ์ต่าง ๆ ที่ตั้งอยู่แบบไม่เลือกที่อันหมายถึงการที่ข้อมูลต่าง ๆ อาจมีโอกาสรั่วไหลตรงจุดไหนของเน็ตเวอร์กก็ได้ นับตั้งแต่ตรงจุดที่เป็นเวอร์กสเตชันจนถึงบริดจ์ และเกตเวย์ต่าง ๆ จนแม้กระทั่งที่ตั้งเคเบิ้ลก็ยังหาความปลอดภัยมิได้ เพราะอาจมีการดักฟังได้อย่างง่ายดายด้วยการใช้ระบบการวิเคราะห์แลน หรือเครื่องดักฟังอื่นในการตรวจจับสัญญาณที่ส่งไปตามสายเคเบิ้ล

การป้อนพาสส์เวิร์ดที่ถูกต้องเข้าไป จุดที่ล่อแหลมต่อความปลอดภัยของข้อมูลอันต่อไปก็จะเป็นเวอร์กสเตชัน ซึ่งถ้ามีการปล่อยปละละเลยเมื่อใดก็อาจจะมีปัญหาในแง่ของการรักษาความปลอดภัยข้อมูลขึ้นได้ เช่น ผู้ใช้บางรายอาจละทิ้งเวอร์กสเตชันไปไหน ๆ โดยที่ยังอยู่ในสภาพการล็อคอินอยู่ ซึ่งถ้าเป็นระบบเน็ตเวอร์กที่มีการควบคุมอย่างดีแล้วจะมีการส่งสัญญาณเป็นเชิงถามหรือให้ผู้ใช้เวอร์กสเตชันแสดงให้ทราบว่า ยังมีคอนเน็คชันกับเน็ตเวอร์กอยู่อีกหรือเปล่าเมื่อเห็นว่าเวอร์กสเตชันตัวใดตัวหนึ่งไม่ได้มีการใช้งานนานเป็นเวลาพอสมควร เมื่อเป็นเช่นนี้ผู้ใช้ที่มีความรับผิดชอบจึงต้องทำการล็อคออฟเน็ตเวอร์กเมื่อเลิกใช้งาน หรือไม่ก็เก็บเวอร์กสเตชันหรือตัวพีซีเข้าตู้ใส่กุญแจเสียเป็นการสิ้นเรื่อง โดยต้องยอมเสียเวลาไปบ้างเพื่อแลกกับความปลอดภัยของข้อมูล

พรินเตอร์ที่ต่อเข้ากับแลนก็จัดเป็นอีกจุดที่ไม่ปลอดภัยในการรักษาความลับ จึงต้องระวังด้วยการไม่ปล่อยให้พรินเตอร์ทำการพิมพ์ข้อความที่เป็นความลับ หรือควรปกปิดในขณะที่เห็นว่าโอกาสที่จะมีผู้คอยเฝ้าดูแลอยู่มีน้อยมาก จากที่ยกตัวอย่างและยังมีอีกหลาย ๆ เรื่องที่เกี่ยวกับระบบการรักษาความปลอดภัยข้อมูลที่จัดเป็นเรื่องต้องระวังกันเอาเอง เพราะไม่มีมาตรการอะไรที่ดีกว่านี้

ความเสี่ยงประการต่อไปเป็นเรื่องของแลนเคเบิล เพราะขณะนี้ได้มีผลิตภัณฑ์ในด้านของเครื่องดักฟังในเน็ตเวอร์กออกมาวางขายมากมายหลายยี่ห้อ ที่มีคุณสมบัติสามารถนำมาใช้วิเคราะห์ระบบการสื่อสารในเน็ตเวอร์ก (และในเวลาเดียวกันถ้ามีผู้ประสงค์จะนำไปใช้ในทางมิชอบก็อาจใช้เครื่องมือเช่นนี้ดักฟังข้อมูลได้ด้วย) เช่น ไอบีเอ็มโทเก้นริงและระบบที่เป็นอีเธอร์เน็ตเน็ตเวอร์ก การลดการเสี่ยงในเรื่องนี้ทำได้โดยใช้สื่อส่งสัญญาณในเน็ตเวอร์กเป็นแบบไฟเบอร์ออปติก แต่ต้องเสียค่าใช้จ่ายสูง รวมทั้งจะมีปัญหาในขณะที่ต้องการจะเปลี่ยนแปลงหรือปรับปรุงเคเบิ้ลแบบนี้ นอกจากนี้แล้วการทำงานของอุปกรณ์อิเล็กทรอนิกส์ทุกอย่างจะปล่อยสัญญาณที่เป็นคลื่นแม่เหล็กไฟฟ้าออกมาด้วย ซึ่งเครื่องดักฟังทั้งหลายจะสามารถรับสัญญาณนี้โดยสะดวกเช่นจากตัวเวอร์กสเตชัน ไม่ว่าเวอร์กสเตชันนี้จะอยู่ในแลนหรือไม่ การดักฟังสัญญาณเช่นนี้ก็จะทำให้ทราบถึงการส่งข้อมูลของเวอร์กสเตชันว่ามีอะไรอยู่นั้นบ้าง นอกเสียจากว่าจะมีการสร้างเกราะคุ้มกันคอมพิวเตอร์หรือเวอร์กสเตชันเพื่อกันให้คลื่นแม่เหล็กไฟฟ้าเล็ดรอดออกมาได้น้อยที่สุด ในเรื่องนี้ก็มีมาตรฐานอันหนึ่งที่เรียกว่า TEMPESTed Standard (ของสหรัฐฯ) ที่ได้กำหนดระดับของการแผ่รังสีหรือคลื่นแม่เหล็กไฟฟ้าให้อยู่ในปริมาณที่จำกัดค่าหนึ่ง ซึ่งจะเป็นประโยชน์ในแง่ของการรักษาความปลอดภัยข้อมูล มาตรฐานอันนี้ก็ได้รับการขานรับและนำไปปฏิบัติโดยผู้ผลิตอุปกรณ์คอมพิวเตอร์หลายรายด้วยกัน เช่น IBM, DEC, Wang ที่ได้นำอุปกรณ์ที่ผลิตตามมาตรฐานของ TEMPESTed ออกจำหน่ายมาหลายปีแล้ว ในอดีตผู้ซื้ออุปกรณ์เหล่านี้ในสหรัฐฯ จะเป็นภาครัฐเสียส่วนใหญ่ แต่ในปัจจุบันภาคเอกชนก็ได้เริ่มหันมาให้ความสนใจเรื่องนี้มากขึ้น เพราะได้เริ่มจะเห็นความสำคัญและปัญหาต่าง ๆ ในด้านการรักษาความปลอดภัยข้อมูลกันมากขึ้น ที่สำคัญก็คือมาตรฐาน TEMPESTed ที่ใช้กับแลนได้ เช่นการกำหนดให้มีการหุ้มสายนำสัญญาณไฟฟ้าเพื่อป้องกันให้การแผ่รังสีมีอยู่ในระดับหนึ่ง แต่วิธีนี้ต้องใช้เงินลงทุนสูง มีผู้ให้ความคิดเห็นว่าในกรณีของแลนนี้น่าจะอาศัยกรรมวิธีที่เรียกว่า ดาต้าเอ็นคริปชันมาใช้จึงจะประหยัดกว่า



ในเรื่องของเอ็นคริปชันมีส่วนที่สำคัญมากอย่างหนึ่งที่จะกล่าวถึงคือ ไฟล์เอ็นคริปชัน อันเป็นขบวนการแปลงไฟล์ต่าง ๆ ให้อยู่ในรูปของรหัส ซึ่งจะต้องถอดรหัสหรือดีคริปชันอีกครั้งที่ปลายทาง เช่นเวอร์กสเตชันและส่วนที่ทำหน้าที่ในการส่งสัญญาณผ่านตัวกลาง สำหรับการที่จะทำการถอดรหัสนั้นจะอาศัยสิ่งที่เรียกว่า ดีคริปชันคีย์ ซึ่งเป็นกุญแจรหัสอย่างหนึ่งที่ผู้ใช้หรือผู้ที่เกี่ยวข้องเท่านั้นที่จะรู้ ผลิตภัณฑ์ที่จะทำหน้าที่เอ็นคริปชันนี้จะอยู่ในรูปของซอฟต์แวร์เป็นส่วนใหญ่และมีราคาค่อนข้างสูง ประกอบกับไม่รับรองว่าจะมีประสิทธิภาพในการทำงานได้เต็มร้อยเปอร์เซ็นต์ เนื่องจากอาจมีปัจจัยหลาย ๆ อย่างที่จะมีผลมาทำให้ข้อมูลหรือดาต้าที่ได้มีการเอ็นคริปต์นี้เกิดการสูญหายได้ รวมถึงการลืมกุญแจของรหัส

ระบบรักษาความปลอดภัยในอุดมการณ์

ในเวลาที่พูดถึงการรักษาความปลอดภัยข้อมูลในเน็ตเวอร์กเช่นในระบบแลนนั้น สิ่งที่เข้ามาเกี่ยวข้องด้วยอย่างมาก ๆ คงหนีไม่พ้นเรื่องของโปรแกรมปฏิบัติการระบบ (Operating System) โดยเฉพาะในส่วนที่เกี่ยวกับคุณลักษณะในส่วนของการรักษาความปลอดภัยข้อมูลที่จะมีผลต่อระบบการรักษาความปลอดภัยข้อมูลในเน็ตเวอร์กอย่างรวม ๆ หลักในการรักษาความปลอดภัยข้อมูลในเน็ตเวอร์กในโลกของไมโครคอมพิวเตอร์นั้น ได้รับอิทธิพลอย่างมากมาจากคุณลักษณะของการรักษาความปลอดภัยข้อมูลในโปรแกรมปฏิบัติการระบบที่มีอยู่ในคอมพิวเตอร์ขนาดใหญ่ เช่น เมนเฟรม และมินิคอมพิวเตอร์ แต่ก็เป็นหลักกว้าง ๆ ที่นำมาใช้ได้ทั่วไปแม้กระทั่งในโลกของพีซี เวอร์กสเตชัน เซอร์ฟเวอร์ ฯลฯ รวมถึงการนำมาใช้ในระบบเน็ตเวอร์กได้อย่างชอบด้วยเหตุผล การทำเน็ตเวอร์ก (เช่น แลน) ให้มีความปลอดภัยจนถึงขั้นอุดมการณ์นั้นจะต้องอาศัยมาตรการหลาย ๆ อย่างประกอบกัน ซึ่งจะกล่าวทีละประเด็นดังนี้

การแสดงตน (User Authentication)

เรื่องแรกในแง่ของการรักษาความปลอดภัยในแลนหรือในเน็ตเวอร์กมักจะหนีไม่พ้นการแสดงตน เพื่อเป็นการพิสูจน์ว่าใครเป็นใคร ซึ่งอาจอาศัยสิ่งที่เรียกว่าพาสส์เวิร์ด จนถึงอุปกรณ์อื่น ๆ เช่น อีพรอมคีย์ และโทเก้นเบสซิสเต็มส์

อีพรอมคีย์เป็นกุญแจพลาสติกอย่างหนึ่งที่มีอีพรอมชิพอยู่ในนั้นและจะทำหน้าที่เก็บเอ็นคริปชันโค้ดเป็นการชั่วคราว ในเวลาใช้งานผู้ใช้ก็จะสอดคีย์หรือกุญแจนี้เข้าไปในช่องเล็ก ๆ ซึ่งอยู่ติดกับ NIC (Network Interface Card) ของเวอร์กสเตชัน จากจุดนี้ก็จะมีการอ่านโค้ดจากคีย์เข้าไปในเครื่องและส่งไปให้หน่วยควบคุมการรักษาความปลอดภัเพื่อทำการพิสูจน์ และในการใช้งาอีพรอมคีย์แต่ละครั้งนี้จะมีการอัพเดโค้ดในคีย์และในหน่วยควบคุมพร้อมกันไป และถ้าผู้ใช้พยายามจะนำคีอันเดียวกันนี้ไปใช้ในเวอร์กสเตชอื่น ๆ ที่ไม่มีสิทธิใช้ สิ่งที่อยู่ในอีพรอก็จะถูกลบไปทันที พร้อม ๆ กับสัญญาณแจ้งภัยดังขึ้นที่ระบบควบคุการรักษาความปลอดภัย

รูปที่ 2 การรักษาความปลอดภัยในเน็ตเวอร์กยุคปัจจุบันที่ได้ก้าวมาถึงขั้นที่มีผลิตภัณฑ์ที่เป็นการรักษาความปลอดภัยในแลน ซึ่งสามารถสนองความต้องการอันเข้มงวดของหน่วยงานเช่น กระทรวงกลาโหมของสหรัฐฯ ได้ (DOD Grade Security)

ในกรณีของไทเก้นเบสซิสเต็มส์นั้นผู้ใช้จะมีสิ่งที่เรียกว่า "เครื่องคิดเลข" ขนาดเท่าบัตรเครดิตให้ถือไว้เป็นกรรมสิทธิ์และเมื่อผู้ใช้ต้องการจะล็อคออนกับเน็ตเวอร์ก เน็ตเวอร์กก็จะแสดงตัวเลขอันหนึ่งออกมา ซึ่งผู้ใช้จะคีย์ตัวเลขดังกล่าวเข้าไปในเครื่องคิดเลข และเครื่องคิดเลขก็จะแสดงตัวเลขตัวที่สองออกมาให้ผู้ใช้เพื่อใช้เลขตัวที่สองนี้ไปทำการเข้าสู่เน็ตเวอร์กต่อไป อุปกรณ์ที่จะใช้การแสดงตนนี้มีมากมายหลายแบบ รวมทั้งที่เป็นแบบไฮ-เทคซึ่งจะมาสัมผัสวัดตรวจสอบรูปร่างหน้าตาหรือส่วนสำคัญอื่น ๆ (เช่น รอยนิ้วมือ เสียงพูด เป็นต้น) ของผู้ที่จะเข้าไปใช้เน็ตเวอร์กและมีจำหน่ายอยู่แล้วในปัจจุบัน อันรวมไปถึงการใช้วิทยาการในด้านปัญญาประดิษฐ์หรือ AI เข้าช่วยในการวิเคราะห์ลักษณะความหนักเบาในการกดปุ่มเป็นพิมพ์เพื่อแสดงตนเองเป็นต้น

สุดท้ายก็เป็นเรื่องของพาสส์เวิร์ด (password) ที่ถือว่าเป็นกรรมวิธีในการแสดงตนที่เก่าแก่ที่สุดวิธีหนึ่ง ซึ่งในเรื่องของแลนนั้นได้มีผู้ตั้งข้อสังเกตในทางปฏิบัติว่า กฎข้อแรกสำหรับการเข้าไปใช้แลนนั้นจำเป็นต้องให้ผู้ใช้แสดงตนหรือพิสูจน์ตนด้วยพาสส์เวิร์ด คือ จำเป็นต้องพิมพ์รหัสประจำตัวเฉพาะบุคคล (ID) และพาสส์เวิร์ดเข้าไปทุกครั้งก่อนเข้าไปสู่เน็ตเวอร์ก ID นี้อาจมาจากชื่อของผู้ใช้ จนถึงการกำหนด ID โดยอาศัยเอกลักษณ์ของอุปกรณ์หรือเครื่องคำนวณที่จะเข้าไปใช้ หรือบางทีก็ใช้ชื่อของโหมดแทนชื่อของผู้ใช้ ซึ่งวิธีนี้จะต้องมีข้อแม้ว่าผู้ใช้เป็นผู้เดียวที่ใช้เครื่องคำนวณ (เช่น เวอร์กสเตชัน) ทุกวันโดยไม่มีการเปลี่ยนแปลง ในทางปฏิบัติจริง ๆ มักเป็นไปไม่ได้อันเนื่องจากว่า จะต้องมีการเปลี่ยนมือกันใช้คอมพิวเตอร์หรือเวอร์กสเตชันอยู่บ่อย ๆ จึงต้องหันไปใช้มาตรการอื่น ๆ

พาสส์เวิร์ดที่ดีจะต้องประกอบด้วยสัญลักษณ์อักษรต่าง ๆ ไม่น้อยกว่า 6 หรือ 7 ตัวอักษร เพราะจะทำให้เดาได้ยากมาก ๆ ขั้นต่อไปนี้ก็คือว่าควรมีการพิมพ์พาสส์เวิร์ดเข้าไปทุกครั้งที่มีการแสดงความต้องการออกมาจากเน็ตเวอร์ก รวมทั้งควรมีการเปลี่ยนพาสส์เวิร์ดบ่อย ๆ ตลอดจนกำหนดให้มีการตรวจพิสูจน์ความถูกต้องของพาสส์เวิร์ดด้วยโค้ด เช่น ที่ใช้ในเซอร์ฟเวอร์ เพราะสามารถป้องกันการรวบรัดหลีกเลี่ยงได้ ตัวอย่างในเรื่องนี้เคยมีมาแล้วในระบบปฏิบัติการดอสที่ผู้บุกรุกสามารถผ่าน Validation ของเวอร์กสเตชันไปได้ด้วยการแก้ไขโค้ดบางส่วนเพื่อให้เกิดการรวบรัดไม่ต้องมีการผ่านขั้นตอนในการตรวจสอบ จึงจำเป็นต้องหากรรมวิธีอื่นที่จะมาทำให้การสร้างและการใช้พาสส์เวิร์ดเป็นไปโดยเกิดประสิทธิผลสูงสุดในการรักษาความปลอดภัยข้อมูลในระบบ สรุปแล้วระบบการรักษาความปลอดภัยข้อมูลที่สมบูรณ์แบบนั้นจะต้องครอบคลุมไปถึงการกำหนดว่าผู้ถือครอบครอง ID เป็นผู้มีความจำเป็นในการใช้เวอร์กสเตชันที่เป็นกรรมสิทธิ์ของคน ๆ นั้นโดยตรง เพื่อป้องกันไม่ให้ผู้ที่ไม่เกี่ยวข้องลักลอบดู ID จากการใช้แป้นพิมพ์แล้วนำ ID ดังกล่าวไปใช้ในเวอร์กสเตชันอื่น ๆ ด้วยจุดมุ่งหมายอันมิชอบ นอกจากนี้การเข้าไปสู่แลนนั้นยังน่าจะผ่านจุดสกัดที่จะคอยดูแลในแง่ของความปลอดภัยด้วยการเลือกว่าใครควรมีสิทธิเข้าไปในระบบ จุดสกัดนี้อาจอยู่ในรูปของเกตเวย์ หรือโมเด็มที่อยู่ไกลออกไปเชื่อมโยงอยู่และจะทำหน้าที่อนุญาตให้แต่เฉพาะเวอร์กสเตชันที่อยู่ใกล้ไฟล์เซอร์ฟเวอร์ตัวนั้นมากที่สุดถึงจะมีสิทธิจะใช้ไฟล์ในเซอร์ฟเวอร์นั้นได้

ออดิตติ้ง (Auditing)

มาตรการในการรักษาความปลอดภัยในเน็ตเวอร์กเพื่อให้ได้ผลจริง ๆ จะมีทั้งการป้องกัน การติดตาม และอื่น ๆ พร้อม ๆ กัน จึงขอกล่าวถึงมาตรการอันต่อไปที่เรียกว่า ออดิตติ้ง ซึ่งมีจุดมุ่งหมายว่า กิจกรรมใดก็ตามที่เข้ามาเกี่ยวข้องกับการรักษาความปลอดภัยข้อมูลแล้ว จะต้องมีการติดตามอย่างใกล้ชิดเพื่อป้องกันการล่วงละเมิดต่าง ๆ ดังเช่นการพยายามจะเข้าไปในเน็ตเวอร์กให้ได้ จนถึงการพยายามที่จะเข้าถึงทรัพยากรของระบบที่ป้องกันไม่ให้บุคคลภายนอกเข้าไปใช้ นอกจากนี้การออดิตซึ่งหมายถึงการติดตามเหตุการณ์สำคัญ ๆ ในเน็ตเวอร์ก เช่น ผู้ใช้ที่ใช้คีย์การแสดงตนของตัวเองไปไขเพื่อใช้เวอร์กสเตชันของผู้อื่น ซึ่งจะมีผลให้เกิดสัญญาณแจ้งภัยขึ้นที่หน่วยควบคุมของเจ้าหน้าที่รักษาความปลอดภัย ดังนั้นการติดตามในแง่ของออดิตติ้งนี้จะต้องดูไปถึงการเปลี่ยนแปลงของอุปกรณ์เครื่องมือเครื่องใช้ ตลอดจน

การเปลี่ยนแปลงวิธีรักษาความปลอดภัยในแลนกันบ่อยแค่ไหน และในแต่ละครั้งได้มีการเปลี่ยนแปลงอะไรกันบ้าง เพื่อป้องกันเหตุอุบัติต่าง ๆ ในทุก ๆ ทาง ให้รัดกุมที่สุดเท่าที่จะทำได้

สำหรับเทคโนโลยีที่จะมาสนับสนุนงานในด้านออดิตติ้งก็มี อาทิเช่น เฟิร์มแวร์ที่อยู่ใน NIC จะคอยติดตามการล่วงละเมิดกระทำผิดต่าง ๆ ในแลน แล้วรายงานให้หน่วยควบคุมที่มีหน้าที่รักษาความปลอดภัยทราบ แต่การออดิตนี้ก็สร้างปัญหาในเน็ตเวอร์กได้มากเช่นกัน โดยเฉพาะในแง่ของทรูพุต เพราะการส่งข้อมูลต่าง ๆ ไปยังระบบการรักษาความปลอดภัยข้อมูล หน่วยควบคุมนั้นมีส่วนทำให้เกิดการคับคั่งของข้อมูลในเน็ตเวอร์กได้ นอกจากจะสามารถออกแบบระบบออดิตติ้งให้สามารถใช้ดุลยพินิจในการเลือกสอดส่องเฉพาะกรณีที่เห็นว่าน่าสงสัยจริง ๆ แล้วจึงรายงานไปที่หน่วยควบคุมการรักษาความปลอดภัยทราบ เพื่อลดการคับคั่งในเน็ตเวอร์กให้เหลือน้อยที่สุด

การรักษาความปลอดภัยข้อมูลแบบหลายระดับ (Multilevel Security)

แลนที่ดีจะต้องยอมให้มีการรักษาความปลอดภัยข้อมูลเป็นแบบหลายระดับได้ อันหมายถึงความสามารถในการส่งข้อมูลที่อยู่ในระดับของการปกปิดในขั้นต่าง ๆ โดยใช้สายเคเบิ้ลของแลนเพียงสายเดียวได้โดยไม่ต้องวิตกว่าจะไม่ปลอดภัย ส่วนการทำงานของการรักษาความปลอดภัยข้อมูลแบบหลายระดับนี้จะอาศัยเอ็นคริปชันและใช้คีย์หรือกุญแจต่าง ๆ สำหรับแต่ละระดับของเอ็นคริปชัน อันนี้ก็เป็นเพียงหลักการเท่านั้น ยังเป็นได้ยากสำหรับการนำระบบการรักษาความปลอดภัยข้อมูลแบบหลายระดับนี้มาใช้ในแลน เพราะพีซีที่อยู่ปลายทางจะเป็นตัวทำให้การรักษาความลับเป็นไปอย่างยากที่สุด เรื่องที่สำคัญอีกเรื่องในแง่ของการรักษาความปลอดภัยข้อมูลในแลนก็คือ ข้อต้องการที่จะไม่ให้ใครคนใดคนหนึ่งสามารถควบคุมระบบการรักษาความปลอดภัยข้อมูลทั้งหมดได้ วิธีปฏิบัติสำหรับเรื่องนี้ก็คือการแต่งตั้งให้ผู้ทำหน้าที่เป็นผู้บริหารระบบมีหน้าที่ควบคุมในเรื่องของ

- การกำหนดผู้ใช้ (User Definition)
- การควบคุมการใช้งาน (Access Controls)
- ลักษณะซอฟต์แวร์ที่จะมาใช้งาน (Application Software Configuration)
- ฯลฯ

และแต่งตั้งเจ้าหน้าที่ด้านการรักษาความปลอดภัยข้อมูลขึ้นมาอีกตำแหน่งหนึ่ง ไว้ให้คอยควบคุมดูแลในเรื่อง

- การกำหนดพาสส์เวิร์ดและการบริหารจัดการกับเรื่องของพาสส์เวิร์ด
- จัดกำหนดรูปแบบของกลไกต่าง ๆ ที่จะนำมาใช้ในด้านการรักษาความปลอดภัยข้อมูล
- รับผิดชอบงานด้านออดิตติ้ง

นอกจากนี้ก็จะต้องแน่ใจว่าความรับผิดชอบของผู้บริหารระบบกับเจ้าหน้าที่รักษาความปลอดภัยข้อมูล ไม่ก้าวก่ายซึ่งกันและกัน

ผลิตภัณฑ์ด้านเอ็นคริปชัน

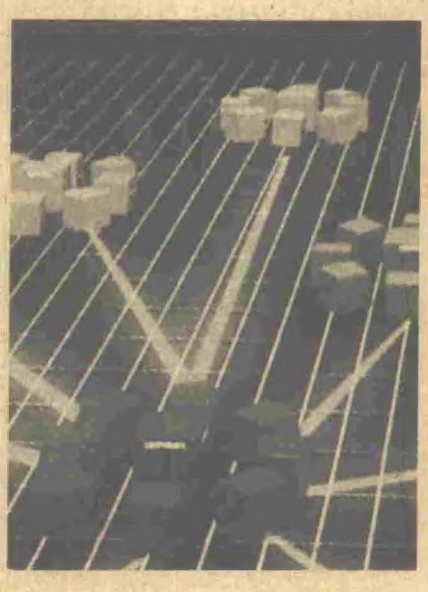
ได้กล่าวถึงเรื่องราวของเอ็นคริปชันมาพอสมควรแล้วว่ามีความสำคัญกับเน็ตเวอร์กอย่างไรบ้าง จึงจะขอกล่าวต่อว่าในแง่ของเอ็นคริปชันนี้ได้เกิดมีผลิตภัณฑ์ทางการค้าอะไรบ้างที่จะมาสนับสนุนกิจกรรมในเรื่องของการสร้างและถอดรหัสข้อมูล ซึ่งจำเป็นต้องอธิบายที่มาของคำสองคำคือ NSA และ DES ให้เข้าใจเสียก่อน

NSA (National Security Agency) นี้ได้ก่อตั้งขึ้นเมื่อปี ค.ศ. 1952 เพื่อรับผิดชอบเกี่ยวกับการสร้างและการถอดรหัสข้อมูลที่ใช้ในงานด้านการป้องกันประเทศสหรัฐอเมริกา หน่วยงานนี้จึงจะมีบทบาทในเรื่องของการเข้ารหัสหรือเอ็นคริปชัน ส่วน DES ตั้งขึ้นเมื่อปี ค.ศ. 1973 เมื่อ National Bureau of Standards (NBS) ของประเทศสหรัฐอเมริกาซึ่งมีหน้าที่รับผิดชอบในเรื่องของการกำหนดมาตรฐานต่าง ๆ ได้รับการร้องเรียนจากหน่วยงานต่าง ๆ ในภาคเอกชนว่า อยากจะให้มีการกำหนดมาตรฐานอะไรขึ้นมาสักอย่างเพื่อไว้สำหรับรักษาความลับของข่าวสารข้อมูลที่ทำการรับ/ส่งด้วยคอมพิวเตอร์ อันทำให้ NBS ต้องออกประกาศให้สถาบันต่าง ๆ ที่เชี่ยวชาญด้านนี้ให้ช่วยกัน

เสนอเทคนิคของการทำดาต้าเอ็นคริปชันที่จะนำไปใช้งานของภาคเอกชนมาให้พิจารณา ซึ่งก็มีผู้เสนอเพื่อขายความคิดนี้อยู่หลายรายด้วยกัน แต่ในที่สุด NBS ก็เลือกดาต้าเอ็นคริปชันเทคนิคของบริษัทไอบีเอ็ม แล้วประกาศเป็นมาตรฐานเมื่อปี ค.ศ. 1977 โดยเรียกว่า Data Encryption Standard (DES) ส่วนวิธีการทำงานของ DES ของไอบีเอ็มนั้น จะมีลักษณะดังนี้คือ ในขณะเอ็นคริปชัน DES อัลกอริธึมจะแบ่งข้อความออกเป็นบล็อก ๆ โดยแต่ละบล็อกจะมีสัญลักษณ์อักษรอยู่ 8 คาแรกเตอร์ แล้วแปลงสิ่งที่อยู่ในแต่ละบล็อกดังกล่าวให้เป็นรหัส โดยทำการแปลงทีละบล็อก ด้วยการสับเปลี่ยนโยกย้ายสิ่งที่อยู่ในแต่ละบล็อกถึง 16 ครั้ง เพื่อให้เกิดเป็นรหัสที่สับสนที่สุดภายใต้การควบคุมของสิ่งที่เรียกว่า คีย์ (Key) จนเกิดเป็นสิ่งที่เรียกว่า eight characters of ciphertext หรือข้อความที่เป็นรหัสที่มีความยาว 8 คาแรกเตอร์

ผลิตภัณฑ์ด้านเอ็นคริปชันนั้นจะใช้มาตรฐานของเอ็นคริปชันอัลกอริธึมตั้งแต่หนึ่งแบบหรือมากกว่านั้น และในกลุ่มของมาตรฐานที่นำมาใช้สร้างเป็นผลิตภัณฑ์นั้นก็จะประกอบด้วยมาตรฐาน DES และมาตรฐาน Rivest Shamir Adleman (RSA) รวมอยู่ด้วย กรรมวิธีในการทำเอ็นคริปชันนี้จะอาศัยชิพเซตชนิดพิเศษที่อยู่บน NIC ซึ่งในระบบที่อยู่บนฐานของ DES (หรือ Private-Key Systems) นั้น จะใช้คีย์เพียงอันเดียวในการสร้างและถอดรหัสข้อมูล ในการใช้งานผู้ส่งข้อมูลจะต้องส่งคีย์อันนี้ไปยังจุดที่อยู่ปลายทางด้วย ส่วนของ RSA นั้นจะเป็นระบบคีย์สาธารณะที่มีคีย์อยู่สองคีย์ เมื่อเวลาจะใช้งานผู้ใช้แต่ละคนก็จะประกาศคีย์สาธารณะให้ทุกคนที่จะส่งข้อมูลที่อยู่ในรูปของรหัสทราบ เพื่อให้สามารถส่งมาถึงตนได้ เสร็จแล้วผู้รับข้อมูลก็จะใช้คีย์ส่วนตัวหรือกุญแจส่วนตัวมาถอดรหัสข้อมูลที่ส่งเข้ามาว่ามีใจความอะไรบ้าง

ในช่วงที่ผ่านมา NSA ได้มีการเปลี่ยนแปลงในด้านของระบบรหัสหลาย ๆ อย่างดังนี้คือ ในปี ค.ศ. 1988 NSA ได้เลิกใช้มาตรฐานที่เรียกว่า DES สำหรับงานด้านการรักษาความปลอดภัยข้อมูลและได้เริ่มให้การแนะนำให้ภาคเอกชนเลิกใช้ DES แล้วหันมาใช้เอ็นคริปชันอัลกอริธึมอันใหม่ที่ NSA ควบคุมอยู่ เพราะอัลกอริธึมที่ NSA ควบคุมอยู่นี้ถือเป็นความลับ ผลิตภัณฑ์ที่อยู่ในการควบคุมของ NSA จึงจำกัดจำนวนอยู่ในวงแคบ ซึ่งกิจกรรมทั้งหมดเท่าที่ได้เล่ามานี้ NSA เรียกโครงการนี้ว่า Commercial COMSEC (Communications Security) - Endorsement Program หรือย่อ ๆ ว่า "CCEP" ที่จะมาทำหน้าที่ประเมินความเชื่อถือได้สำหรับผลิตภัณฑ์ต่าง ๆ ในด้านเอ็นคริปชัน จึงจำเป็นต้องพูดถึงบทบาทของ NSA ในเรื่องนี้สักเล็กน้อย



บทบาทของ NSA

หน้าที่หลักของ NSA ก็คือการกำหนดมาตรฐานในด้านการรักษาความปลอดภัยข้อมูลคอมพิวเตอร์ แต่ขอบข่ายอิทธิพลของหน่วยงานนี้ไม่ได้หยุดอยู่แค่นี้ เพราะในฐานะที่มีนักวิชาการผู้ทรงคุณวุฒิตลอดจนผู้เชี่ยวชาญในสาขาต่าง ๆ ในด้านการรักษาความปลอดภัยข้อมูลประจำอยู่อย่างมากมาย รวมทั้งหน้าที่ที่ NSA ต้องรับผิดชอบนั้นได้เขียนไว้กว้างมากครอบคลุมไปในทุกเรื่องที่เกี่ยวกับการสร้างและการถอดรหัส หรืออะไรก็ตามที่เป็นเรื่องของความมั่นคง จึงน่ามาดูว่าในด้านของคอมพิวเตอร์นั้น NSA ได้ทำอะไรไว้บ้าง NSA ได้ก่อตั้งโครงการต่าง ๆ ที่เกี่ยวกับการประเมินผลการรักษาความปลอดภัยข้อมูลขึ้น เพื่อใช้วัดมาตรฐานความปลอดภัยของคอมพิวเตอร์แบบต่าง ๆ และคอมพิวเตอร์เน็ตเวอร์ก รวมทั้งอุปกรณ์ประมวลข้อมูลอีกมากมายหลายชนิดว่าจะสามารถทนต่อการลักลอบโจรกรรมในด้านตัวเลขข้อมูล และทนต่อการกระทำอันมิชอบต่าง ๆ ได้สักเท่าใด ซึ่งการประเมินผลนี้ได้วิวัฒนาการมาจากแต่เดิมที่มีเพียงสองขั้นตอนให้กลายมาเป็นห้าขั้นตอนในปัจจุบัน ขั้นตอนในการประเมินผลนี้เรียกว่า Rating The Security ซึ่งมีขั้นตอนต่าง ๆ ดังนี้

ขั้นตอนแรก ก่อนทำการออกแบบผลิตภัณฑ์ (คอมพิวเตอร์ คอมพิวเตอร์เน็ตเวอร์ก หรืออุปกรณ์ประมวลผลข้อมูล) นั้น ถ้าผู้ผลิตหรือเว็นเดอร์อยากเข้ามาใช้มาตรฐานของ NSA ก็ต้องเข้ามาทำสัญญาข้อตกลงต่าง ๆ ระหว่างตนกับ NSA เพื่อขอรับการประเมินผล เสร็จแล้วจึงเริ่มออกแบบ

ซึ่งในขณะออกแบบอยู่ก็จะต้องมีการปรึกษาหารือกับ NSA ตลอดเวลาเพื่อให้ทุกอย่างสอดคล้องกับเป้าหมายของการรักษาความปลอดภัยข้อมูลที่วางไว้ จนเมื่อออกแบบเสร็จแล้วก็ถือว่าข้อหารือระหว่างเว็นเดอร์กับ NSA นั้นยุติลงได้ ขั้นต่อไปก็เป็นการสร้างเครื่องหรืออุปกรณ์ต้นแบบแล้วส่งให้ NSA ประเมินผลอย่างเป็นทางการ ในช่วงนี้ทาง NSA จะยอมให้เว็นเดอร์แก้ไขข้อบกพร่องได้นิดหน่อย เพราะทุกอย่างได้ก้าวมาถึงขั้นสุดท้ายอันจะทำการออกแบบใหม่อีกไม่ได้

นอกจากนี้ยังมีการประเมินผลในขั้นที่เรียกว่า Rating Maintenance Phase เป็นข้อกำหนดของ NSA ที่นำมาใช้กับผลิตภัณฑ์บางอย่างของเว็นเดอร์ในกรณีที่เว็นเดอร์ยังจะคงนำผลิตภัณฑ์รุ่นหรือโมเดลต่อ ๆ ไปออกจำหน่ายและให้ผู้ซื้อยอมรับ ส่วนมาตรฐานที่ NSA ใช้ในการประเมินคุณภาพในด้านการรักษาความปลอดภัยข้อมูลของผลิตภัณฑ์ของเว็นเดอร์ ซึ่ง NSA ได้กำหนดไว้มีอยู่ดังนี้คือ

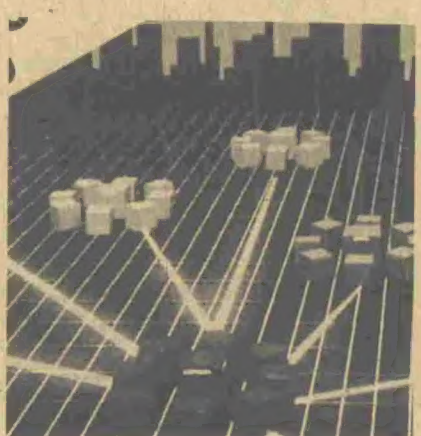
D - ไม่เคยได้รับการประเมินจาก NSA หรือสอบไม่ผ่าน เพราะไม่สามารถทำตามข้อกำหนดขั้นต่ำสุดของ NSA

C - ต้องใช้สิ่งที่เรียกว่า Discretionary Access Control (DAC) และออดิตติ้ง รวมทั้งใช้การแสดงตนเพื่อกำชับนโยบายในด้านการรักษาความปลอดภัยข้อมูล

B - ให้เพิ่ม Mandatory Access Control (MAC) เพื่อเพิ่มความแข็งแกร่งในด้านการรักษาความปลอดภัยข้อมูล

A - เหมือน B ในหลักการแต่กลไกต่าง ๆ ที่เกี่ยวกับการรักษาความปลอดภัยข้อมูลได้รับการประเมินผลอย่างละเอียดและเข้มงวดมากขึ้น

งานอื่น ๆ ของ NSA ก็ยังมีอาทิเช่น ฮาร์ดแวร์เอ็นคริปชันที่ส่งมาให้ NSA อนุมัติ รวมทั้งคอมพิวเตอร์ที่มีระบบการรักษาความปลอดภัยข้อมูลสูงที่เรียกว่า TEMPEST Computers และบริการต่าง ๆ ในด้านการสื่อสารโทรคมนาคม ซึ่งจะได้อธิบายให้ทราบถึงความหมายของ DAC และ MAC อันเป็นมาตราการที่ใช้ในการควบคุมตัวบุคคลในเรื่องของการเข้าไปหาหรือเข้าไปใช้สิ่งใดสิ่งหนึ่ง (เช่น ข้อมูล) ซึ่งเป็นข้อกำหนดของ TCSEC (Department of Defense Trusted Computer System Evaluation Criteria) และ TNI (Trusted Network Interpretation) เป็นข้อกำหนดที่เกิดจากฝีมือของ NSA ในปี ค.ศ. 1983 และ 1987 ตามลำดับ ส่วน DAC นั้นหมายถึงข้อบังคับสำหรับผู้ใช้ที่จะสามารถเข้าถึงข้อมูลหรือทรัพยากรเครื่องใช้บางอย่างได้ โดยดูจากว่าผู้ใช้อยู่ในฐานะใด อันนี้ก็เป็นการกรองขั้นแรก ขั้นต่อไปก็จะเป็นมาตราการที่เข้มงวดเข้าไปอีกคือ MAC ที่มีความหมายสั้น ๆ ว่า "ใคร" สมควรที่จะดูหรือรู้เรื่องอะไร ซึ่งจะมีการกำหนดลงไปอย่างตายตัวว่าใครควรรู้สิ่งนั้นสิ่งนี้เป็นเฉพาะรายการหรือเป็นเฉพาะเรื่องและจะผิดจากนี้ไม่ได้เป็นอันขาด



อแวร์เน็ต (Aware Net)

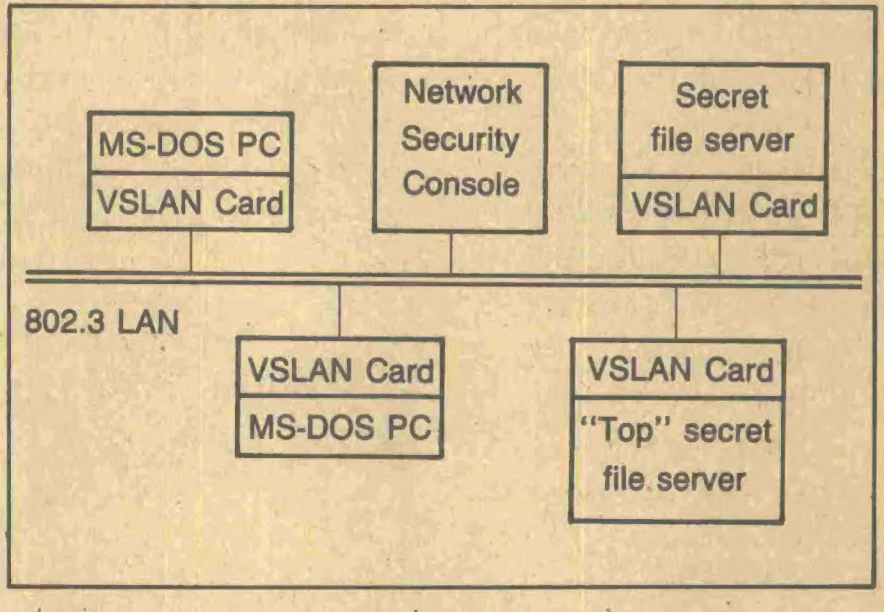
ในยุคแรก ๆ ราวปี ค.ศ. 1987 ผลิตภัณฑ์ทางด้านแลนที่นำหลักการของการรักษาความปลอดภัยข้อมูลเข้ามาใช้ในการออกแบบหรือในการทำส่วนประกอบต่าง ๆ ยังมีน้อยมาก แต่ความต้องการในการใช้งานผลิตภัณฑ์ประเภทนี้ก็ได้มีมานานพอสมควรทั้งในภาครัฐ (เช่น กระทรวงกลาโหม) และภาคเอกชนของประเทศสหรัฐอเมริกา อันทำให้เกิดมีบริษัทที่ปรึกษาต่าง ๆ ขึ้นมา เช่น บริษัท Riverbend Group Inc. ที่เชี่ยวชาญในด้านแลนซิสเต็มส์อินติเกรชันและการพัฒนาซอฟต์แวร์สำหรับแลน เป็นผู้ริเริ่มโครงการซิสเต็มส์อินติเกรชันขึ้นมา โดยมีจุดมุ่งหมายที่จะสร้างแลนบนฐานพีซีที่นำเอาเรื่องของการรักษาความปลอดภัยข้อมูลเข้ามาผนวกไว้ ซึ่งจะสามารถสนองข้อต้องการของกระทรวงกลาโหมของสหรัฐฯ รวมทั้งภาคเอกชนอีกหลาย ๆ รายให้อยู่ภายใต้มาตรฐานของ NSA มากที่สุด เพื่อให้เป็นที่ยอมรับของผู้ใช้ และในขณะเดียวกันก็ต้องสนับสนุนการใช้งานเอ็มเอสดอสพร้อมกันไปด้วย ระบบการรักษาความปลอดภัยข้อมูลในแลนที่บริษัทรีเวอร์เบนด์สร้างขึ้นมานั้นเป็นผลงานที่น่าสนใจที่สุดอย่างหนึ่งในการพยายามที่จะใช้พีซีแบบต่าง ๆ ที่มีอยู่ในท้องตลาดของประเทศสหรัฐอเมริกาในขณะนี้ทำหน้าที่เป็นเวอร์กสเตชันและไฟล์เซอร์ฟเวอร์ ขั้นต่อไปก็เป็นการมองหา Network Operation System (NOS) ที่จะมาบริหารจัดการตัวเน็ตเวอร์ก รวมทั้งการจัดการในเรื่องของการใช้พรินเตอร์และการใช้ไฟล์ร่วมกัน เป้าหมายของรีเวอร์เบนด์จึงมีว่าจะต้องสร้างผลิตภัณฑ์

เน็ตเวอร์กที่สามารถสนับสนุนการรักษาความปลอดภัยข้อมูลในแบบหลายระดับ เพื่อใช้กับพีซีที่มีระบบปฏิบัติการเอ็มเอสดอส นอกจากนั้นรีเวอร์เบนด์ได้เลือกใช้ NOS ที่ NSA ยังไม่ให้การยอมรับ โดยนำไปใช้กับฮาร์ดแวร์ของพีซีที่เป็นแบบธรรมดา ๆ ซึ่งมีขายทั่วไป ดังนั้นรีเวอร์เบนด์ต้องมีเหตุผลอย่างหนักแน่นในทุกขั้นตอนว่าทำไมจึงทำอย่างนั้นอย่างนี้ กว่าจะได้มาซึ่งระบบการรักษาความปลอดภัยในแลนที่ใคร ๆ ยอมรับ

ขั้นแรกสำหรับรีเวอร์เบนด์จะเป็นการเลือกระบบปฏิบัติการสำหรับเน็ตเวอร์ก (NOS) ซึ่งได้มีการตัดสินใจเลือกใช้เน็ตแวร์ของบริษัทโนเวลล์ อันเนื่องจากว่าเป็น NOS ที่ได้รับความสำเร็จอย่างสูงในท้องตลาดปัจจุบัน เพราะเน็ตแวร์มีระบบรักษาความปลอดภัยข้อมูลในขณะใช้งานอยู่ในระดับความพอใจในทางธุรกิจการค้าในชื่อของผลิตภัณฑ์ว่า NetWare 2.15 ในเน็ตแวร์ 2.15 (รวมทั้ง NetWare 386) สามารถให้การรักษาความปลอดภัยข้อมูลในด้านการควบคุมใช้งาน และเอ็นคริปต์พาสส์เวิร์ด รวมทั้งกลไกที่จะทำให้แน่ใจว่าผู้ใช้เปลี่ยนพาสส์เวิร์ดอย่างสม่ำเสมอ

ในขั้นต่อมารีเวอร์เบนด์ก็มาพิจารณาเลือกเวอร์กสเตชัน ซึ่งโดยตัวของมันเองแล้วไม่ปลอดภัยในการที่จะรักษาความปลอดภัยของข้อมูล จึงต้องหาอุปกรณ์อะไรสักอันมาวางระหว่างแต่ละเน็ตเวอร์กโหนดเพื่อควบคุมการสื่อสารจากเวอร์กสเตชันหนึ่งไปยังอีกเวอร์กสเตชันหนึ่ง และจากเวอร์กสเตชันไปยังไฟล์เซอร์ฟเวอร์ จึงได้พิจารณาเลือกผลิตภัณฑ์ที่เรียกว่า VSLAN ของบริษัท Verdix Corp. ที่ประกอบธุรกิจในลักษณะ Original Equipment Manufacturer (OEM) ให้มาทำหน้าที่ในการควบคุมต่าง ๆ ขณะที่พิจารณาเลือก VSLAN ใน 1-2 ปีที่ผ่านมานั้น ได้ปรากฏต่อมาว่า ผลิตภัณฑ์ตัวนี้กำลังจะมีการส่งมอบให้ NSA ทำการประเมินผลในแง่ของระบบการรักษาความปลอดภัยข้อมูลในปี ค.ศ. 1990 ผลิตภัณฑ์ VSLAN นี้เป็นการรวม NIC ชนิดต่าง ๆ ที่ทำหน้าที่เฉพาะพิเศษให้เข้ากับการรักษาความปลอดภัยข้อมูลในเน็ตเวอร์กคอนโซล และจะทำหน้าที่เป็น "ยาม" สำหรับการรักษาความปลอดภัยข้อมูลในระบบแลน VSLAN ได้ใช้วิธีการของ TNI พร้อมด้วยดาต้าเอ็นคริปชัน และการแสดงตนที่ควบคุมด้วยกุญแจพกติดตัวไปไหนมาไหนได้ ด้วยคุณสมบัติพิเศษทางสถาปัตยกรรมของ VSLAN นั้นได้ยอมให้แลนฮาร์ดแวร์และองค์ประกอบที่เป็นซอฟต์แวร์ต่าง ๆ ไม่จำเป็นต้องมีระบบรักษาความปลอดภัยข้อมูลโดยมาตรฐานของ NSA กำหนดตราบเท่าที่แต่ละเวอร์กสเตชันและไฟล์เซอร์ฟเวอร์ถูกจำกัดให้อยู่ในระดับการรักษาความปลอดภัยข้อมูลระดับใดระดับหนึ่ง หรืออยู่ในพื้นที่จำกัดอันหนึ่ง ทั้งหมดนี้ก็เป็นขั้นแรกในเรื่องของ VSLAN ที่รีเวอร์เบนด์นำมาใช้อินติเกรตเข้ากับผลิตภัณฑ์ของตนและให้ชื่อใหม่ว่า อแวร์เน็ต (Aware Net) ซึ่งได้แสดงสถาปัตยกรรมไว้ในรูปที่ 3 ส่วนผลิตภัณฑ์ของรีเวอร์เบนด์ที่จะออกจำหน่ายในขั้นต่อไปนั้นก็จะเกิดจากการใช้ซับเซตของผลิตภัณฑ์ของ Verdix เข้ามาร่วมกันกับการใช้ประโยชน์จาก VSLAN เป็นผลิตภัณฑ์ที่มีรูปแบบที่ซับซ้อนขึ้น โดยที่สามารถใช้คอมพิวเตอร์ที่ไม่ต้องผูกอยู่กับเอ็มเอสดอสและสามารถสนับสนุนข้อระบบการรักษาความปลอดภัยข้อมูลในแบบหลายระดับ

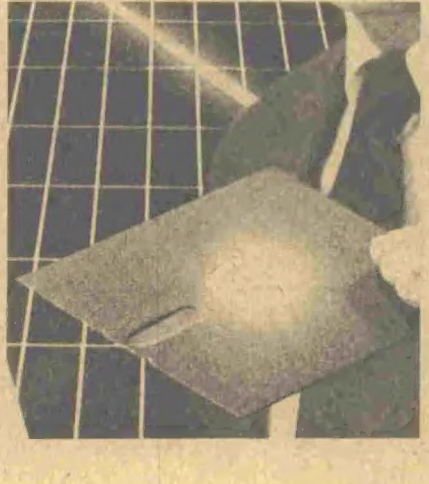
เมื่อจบเรื่องของการเลือกส่วน



รูปที่ 3 สถาปัตยกรรมของ "อแวร์เน็ต" (Aware Net) ที่สามารถให้การสนับสนุนระบบการรักษาความปลอดภัยในแลนแบบหลายระดับ ซึ่งเป็นผลิตภัณฑ์ของบริษัทรีเวอร์เบนด์กรุ๊ป

ประกอบต่าง ๆ ที่จะมาใช้ในอแวร์เน็ตเรียบร้อยแล้ว ก็มาถึงเรื่องของการพัฒนาซอฟต์แวร์ที่จะใช้เชื่อมโยงฮาร์ดแวร์ของ VSLAN ให้เข้ากับเน็ตแวร์ อันทำให้ทีมผู้พัฒนาซอฟต์แวร์ต้องพยายามมองหาทางที่จะทำให้อแวร์เน็ตมีความสมบูรณ์ที่สุด ทั้งในแง่ของการให้บริการการใช้งานในด้านต่าง ๆ จนถึงเรื่องของระบบการรักษาความปลอดภัยของข้อมูล เมื่อเป็นเช่นนี้จึงต้องทำการสร้างซอฟต์แวร์ขึ้นมาเพื่อให้สามารถอุดรูรั่วและขจัดสิ่งที่เป็นจุดอ่อนต่าง ๆ จากผลิตภัณฑ์อื่นที่นำมาประกอบกันเป็นอแวร์เน็ต ซึ่งจะมีทั้งซอฟต์แวร์และฮาร์ดแวร์สำเร็จรูปดังได้กล่าวในตอนต้น จึงจะขอนำข้อบกพร่องของผลิตภัณฑ์ดังกล่าวมาเล่าทีละประเด็นว่ามีอะไรบ้าง ปัญหาอันแรกเป็นเรื่องของเน็ตแวร์ที่ผู้พัฒนาซอฟต์แวร์ของรีเวอร์เบนด์เห็นว่ามีหลาย ๆ จุดที่ต้องปรับปรุง อันเนื่องมาจากว่าสถาปัตยกรรมตลอดจนพฤติภาพการใช้งานของเน็ตแวร์นั้นถึงแม้ว่าจะปลอดภัยต่อข้อมูลตามมาตรฐานของการใช้งานในทางธุรกิจเป็นส่วนใหญ่ก็ตาม แต่ก็มีข้อเสียตรงที่มีความยืดหยุ่นเกินไปอันเนื่องมาจากผู้พัฒนาเน็ตแวร์ต้องการจะทำให้ซอฟต์แวร์นี้ใช้ได้กับแลนฮาร์ดแวร์ให้ได้กว้างที่สุดเท่าที่จะทำได้ ปัญหาอันที่สองเป็นส่วนผลิตภัณฑ์ของ Verdix ในรูปของ NIC ที่เป็นส่วนหนึ่งของอแวร์เน็ตนั้นจะอยู่ในรูปของฮาร์ดแวร์ที่ใช้เทคโนโลยี 802.3 ของ IEEE ซึ่งผิดแผกจากทั่ว ๆ ไปในแง่ที่ว่าเป็นอินเทลลิเยนต์ฮาร์ดแวร์ที่มีไมโครโปรเซสเซอร์อยู่บนบอร์ด พร้อมด้วยโปรเทคเต็ดแรมและเอ็นคริปชันยูนิตหนึ่งตัว ส่วนโปรเทคเต็ดแรมดังกล่าวได้สร้างปัญหาในแง่ที่ว่าจะทำให้พีซีแอกเซสไม่ได้ เมื่อเป็นเช่นนี้ทางรีเวอร์เบนด์ก็ต้องพัฒนาซอฟต์แวร์ขึ้นมาเพื่อเข้าไปแก้ไขปัญหาทั้งสองข้อที่กล่าวมาส่วนหนึ่งเพื่อให้สามารถเชื่อมโยงเน็ตแวร์ TPX calls ต่าง ๆ ให้เข้ากับรายการต่าง ๆ ที่ใช้ได้กับ VSLAN NIC อันทำให้ต้องวางแผนสร้างซอฟต์แวร์อย่างรอบคอบ เพราะถ้าเกิดผิดพลาดขึ้นแม้แต่น้อยก็จะทำให้เกิดปัญหาได้ทันที เช่น อาจเกิดภาวะอาการต่าง ๆ ที่จะเข้ามาล่วงละเมิดระบบรักษาความปลอดภัยข้อมูลของเน็ตเวอร์กได้อย่างง่ายดาย ทั้งหมดนี้ก็เป็นการแก้ปัญหาด้วยซอฟต์แวร์ที่รีเวอร์เบนด์เป็นผู้ลงมือทำเอง ก่อนที่จะกลายเป็นผลิตภัณฑ์สำเร็จรูปที่เรียกอแวร์เน็ตในที่สุด

ระบบอแวร์เน็ตนี้สามารถดูแลเวอร์กสเตชันได้ 56 ตัวกับไฟล์เซอร์ฟเวอร์ได้อีก 8 ตัว พร้อมทั้งสามารถทำให้เกิดมีระดับของการรักษาความปลอดภัยข้อมูลได้ 8 ระดับ ซึ่งในขณะใช้งานนั้น ผู้ใช้ที่อยู่ในระบบการรักษาความปลอดภัยข้อมูลระดับใดระดับหนึ่งจะสามารถเปลี่ยนระดับที่เวอร์กสเตชันของตนได้ด้วยการรีบูตด้วยอีพรอมเอ็นคริปชันคีย์ ทั้งหมดนี้ก็เป็นเรื่องราวของอแวร์เน็ตของบริษัทรีเวอร์เบนด์



กรุ๊ป อันจัดเป็นผลิตภัณฑ์ในด้านการรักษาความปลอดภัยข้อมูลในแลนที่อยู่ในยุคแรก ส่วนผลิตภัณฑ์ในกลุ่มเดียวกันนี้ที่จัดว่าอยู่ในยุคแรกที่เห็นว่าน่าสนใจก็จะมี อาทิเช่น IONET Secure LAN ของ DCA ซึ่งจะกล่าวถึงต่อไป ส่วนราคาค่าใช้จ่ายของอแวร์เน็ตนั้นไม่ได้บอกไว้ แต่ก็คาดว่าคงจะสูงเพราะสร้างขึ้นมาเพื่อให้ได้มาตรฐานที่ทางการของสหรัฐฯ ยอมรับ

หลักในการเลือกซีเคียวแลน (เช่น IONET Secure Lan ฯลฯ)

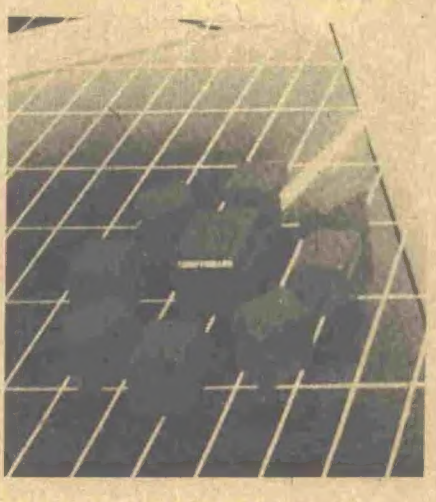
ผลิตภัณฑ์ (เช่น ไอโอเนตซีเคียวแลน) นี้จะมาในรูปของฮาร์ดแวร์และซอฟต์แวร์ที่ต้องใช้ร่วมกับผลิตภัณฑ์อีกตัวหนึ่งของ DCA ที่เรียกว่า DCA IONET Plus network operating system จัดเป็นซอฟต์แวร์ที่มีระบบรักษาความปลอดภัยข้อมูลอยู่ในนั้นบ้างแล้ว แต่เมื่อนำมาใช้ร่วมกับไอโอเนตซีเคียวแลนก็จะทำให้สามารถอุดช่องโหว่ต่าง ๆ ในด้านความปลอดภัยได้เกือบหมดจนอยู่ในขั้นที่กระทรวงกลาโหมของสหรัฐฯ ยอมรับ จะขอกลับมาที่ไอโอเนตพลัสอีกนิดว่าเป็น NOS ซอฟต์แวร์ที่ให้การสนับสนุนเน็ตไบออสที่เป็นมาตรฐานของอุตสาหกรรม และใช้ได้กับอีเธอร์เนตและโทเก้นริงแลน โดย DCA ได้ผลิต NIC การ์ดชนิดต่าง ๆ ไว้สำหรับใช้กับอีเธอร์เนตที่ใช้สายไฟแบบหนาและบาง รวมทั้งอีเธอร์เนตแลนที่ใช้ไฟเบอร์ออปติกเคเบิ้ล นอกจากนี้ทั้งดีซีเอไอโอเนตพลัสและไอโอเนตซีเคียวแลนยังใช้ได้กับ NIC ที่ทำตามมาตรฐานอุตสาหกรรมอื่น ๆ ได้อีกด้วย

สิ่งที่น่าสนใจสำหรับไอโอเนต

ซีเคียวแลนก็คือการเป็นผลิตภัณฑ์ที่เหมาะกับผู้ใช้ เช่น กระทรวงกลาโหมของสหรัฐฯ หรือหน่วยงานอื่นที่มีความเข้มงวดกวดขันในเรื่องของระบบการรักษาความปลอดภัยข้อมูลในเน็ตเวอร์ก เพราะเป็นผลิตภัณฑ์ที่ไม่ขึ้นกับโปรโตคอลตัวใดตัวหนึ่งโดยเฉพาะ รวมทั้งการจัดการในด้านการควบคุมการใช้งานที่เป็นอิสระไม่ขึ้นกับ NOS แต่อย่างใด นอกจากนี้ระบบเอ็นคริปชันของไอโอเนตซีเคียวแลนนี้ทำงานโดยอยู่เหนือชั้นเน็ตไบออส อันทำให้สามารถใช้ผลิตภัณฑ์ตัวนี้กับเกตเวย์และรูตเตอร์แบบที่ใช้กันอยู่ทั่ว ๆ ไปได้ คราวนี้ก็มาถึงเรื่องของค่าใช้จ่ายสำหรับผลิตภัณฑ์ของ DCA ที่คิดราคาไว้ดังนี้คือ ดีซีเอไอโอเนตซีเคียวแลนราคา 1,595 เหรียญสหรัฐฯ (ต่อผู้ใช้หนึ่งราย) และไอโอเนตพลัสสำหรับเน็ตไบออสจะมีราคา 195 เหรียญสหรัฐฯ (ต่อผู้ใช้หนึ่งราย)

เมื่อพูดถึงผลิตภัณฑ์ในด้านการรักษาความปลอดภัยข้อมูลในแลนของผู้ผลิตที่เป็นรายใหญ่ ๆ เช่น รีเวอร์เบนด์กรุ๊ปกับ DCA นั้น เมื่อเราต้องการคิดจะซื้อผลิตภัณฑ์ในด้านการรักษาความปลอดภัยข้อมูลในแลน ควรนึกถึงเรื่องอะไรบ้างดังข้อพิจารณาต่อไปนี้

- ระบบหรือผลิตภัณฑ์ที่เกี่ยวกับการรักษาความปลอดภัยข้อมูลนี้อยู่บนฐานของฮาร์ดแวร์หรือซอฟต์แวร์
- เมื่อได้รับการรบกวนหรือถูกจู่โจมจากผู้ประสงค์ร้ายระบบเช่นนี้จะสามารถทำลายตัวของมันเองหรือไม่
- ผลิตภัณฑ์ในการแสดงตนอันหมายถึงว่าระบบรักษาความปลอดภัยได้ใช้วิธีการอันรัดกุมและปลอดภัยในการพิสูจน์สิทธิของผู้ใช้หรือเปล่า
- เมื่อได้ผ่านขั้นการแสดงตนมาแล้วก็มาถึงขั้นการควบคุมการใช้งานนั้น ผู้ทำผลิตภัณฑ์ด้านการรักษาความปลอดภัยในแลนได้เลือกใช้วิธีใดวิธีหนึ่งใน 4 วิธีนี้หรือเปล่า คือ
  - ก. discretionary access control
  - ข. mandatory access control
  - ค. compartmentation of data
  - ง. division of responsibility
- การออดิตดิ้งระบบการรักษาความปลอดภัยข้อมูลมี activity log หรือมี audit trail สำหรับผู้ใช้ทุกคนหรือไม่ และ audit file นั้นจะปลอดภัยจากการจู่โจมทำลายหรือเปล่า
- transmission security ภายในระบบได้มีวิธีที่จะทำให้การส่งข้อมูลระหว่างจุดต่าง ๆ ในแลนหรือระหว่างแลนเป็นไปอย่างปกปิดหรือเปล่า
- network security administration การบริหารจัดการด้านการรักษาความปลอดภัยข้อมูลทำได้ง่ายแค่ไหน ตลอดจนว่าตัวเลขระบบรักษาความปลอดภัยข้อมูลเองนั้นจะปลอดภัยจากการบุกรุกแค่ไหน
- การเข้ากันได้ของอินเตอร์เฟสที่อยู่ระหว่างสภาพแวดล้อมที่มีระบบการรักษาความปลอดภัยของข้อมูลอยู่กับสภาพแวดล้อมที่ไม่มีระบบการรักษาความปลอดภัยนั้น ได้มีอุปกรณ์เครื่องใช้ที่จะทำหน้าที่โอนถ่ายข้อมูลระหว่างสภาพแวดล้อมที่รักษาความปลอดภัยและไม่รักษาความปลอดภัยหรือเปล่า และได้มีวิธีการที่จะสงวนอุปกรณ์เครื่องมือดังกล่าวไว้ให้บุคคลผู้มีสิทธิโดยเฉพาะหรือไม่
- ระบบการรักษาความปลอดภัยข้อมูลได้ถูกสร้างขึ้นมาตามมาตรฐานอันใดอันหนึ่ง เช่น DES, CCITT หรือ IEEE ที่จะทำให้การใช้งานตลอดจนบำรุงรักษาได้ง่ายหรือเปล่า และมียูทิลิตี้หรือเมนูโปรแกรมให้มาด้วยหรือไม่ ตลอดจนว่ามีระบบอิเล็กทรอนิกส์เมลที่รักษาความปลอดภัยหรือเปล่า นอกจากนี้ยังต้องดูต่อไปอีกว่าเมื่อจบระบบรักษาความปลอดภัยอย่างรวม ๆ แล้วได้ทำหน้าที่ต่าง ๆ ดังได้กล่าวไว้ในข้างต้นได้อย่างปลอดภัยหรือเปล่า ตลอดจนความสะดวกในการใช้ระบบรักษาความปลอดภัยข้อมูลและเรื่องของราคาค่าใช้จ่ายที่ต้องลงทุนไป



มาตรการต่าง ๆ ที่กำหนดขึ้นในการพิจารณาเลือกผลิตภัณฑ์รักษาความปลอดภัยข้อมูลในแลน อันมาจากเหตุผลหลาย ๆ อย่างประกอบกัน เรื่องแรกก็จะเกี่ยวกับการเป็นฮาร์ดแวร์หรือซอฟต์แวร์ของตัวผลิตภัณฑ์ จึงต้องเริ่มที่ประวัติว่าผลิตภัณฑ์ส่วนใหญ่ในด้านการรักษาความปลอดภัยข้อมูลในแลนจะอยู่บนฐานของซอฟต์แวร์ทั้งสิ้น ซึ่งมีข้อเสียอยู่มาก ไม่ว่าการรักษาความปลอดภัยเช่นนี้จะอยู่บนฐานยูนิกซ์ โอเอสทูหรือดอส เพราะการรักษาความปลอดภัยที่อาศัยแต่เพียงซอฟต์แวร์นั้นจะเต็มไปด้วยช่องโหว่ที่โดนแกะรอยได้ง่าย แต่สำหรับกรณีของคอมพิวเตอร์ขนาดกลางและขนาดใหญ่เช่นมินิคอมพิวเตอร์และเมนเฟรมนั้น จะมีระบบรักษาความปลอดภัยที่อาศัยทั้งฮาร์ดแวร์และซอฟต์แวร์ ซึ่ง

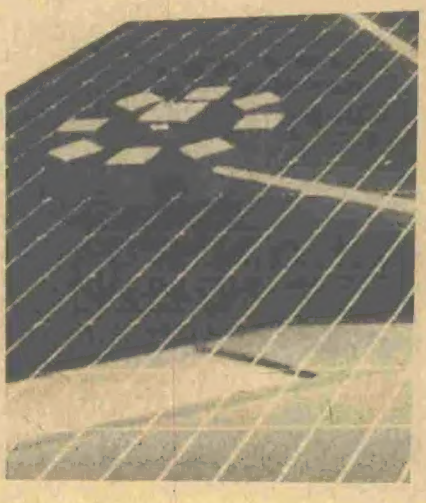
ทำให้เกิดผลดีในแง่ที่ว่าถ้าจะนำซอฟต์แวร์ไปใช้กับฮาร์ดแวร์ที่ไม่เหมาะสมหรือฮาร์ดแวร์ถูกบุกรุกรู้โจม ซอฟต์แวร์ก็จะไม่ทำงาน ในทำนองเดียวกัน ถ้านำฮาร์ดแวร์ไปใช้กับซอฟต์แวร์ที่ไม่เหมาะสมหรือมีการกระทำที่มิชอบกับตัวซอฟต์แวร์ ฮาร์ดแวร์ก็จะไม่ทำงานเช่นกัน ส่วนการสามารถทำลายตัวเอง (self-destruction) นี้ก็เป็นเรื่องจะต้องสามารถทำลายตัวเองหรือทำให้ตัวของมันเองใช้การไม่ได้อีกต่อไปเมื่อถูกบุกรุกรู้โจม ฯลฯ

ผลิตภัณฑ์ย่อยในด้านการรักษาความปลอดภัยข้อมูลในแลน

การปรับปรุงแลนให้มีระบบการรักษาความปลอดภัยข้อมูลมากขึ้นนั้นทำได้หลายทางและไม่จำเป็นต้องลงทุนจนเกินกำลังแต่อย่างใด เพราะขณะนี้ได้มีผลิตภัณฑ์อยู่หลายอย่างที่มีราคาย่อมเยาและจะเข้ามาช่วยในเรื่องนี้ได้ ซึ่งเมื่อมองอย่างกว้าง ๆ แล้วลักษณะการทำหน้าที่ของผลิตภัณฑ์พวกนี้จะแบ่งออกเป็นสองสายใหญ่ ๆ ด้วยกันคือ

1. ผลิตภัณฑ์ทางด้านการแสดงตน

วิธีเพิ่มซีเคียวริตี้ให้แลนและเวอร์กสเตชันที่ตั้งอยู่เดี่ยว ๆ ที่นิยมกันมากที่สุดวิธีหนึ่งเห็นจะเป็นการใช้ผลิตภัณฑ์ในด้านการแสดงตน ซึ่งในกรณีที่นำมาใช้กับพีซีก็จะประกอบด้วยพีซีหนึ่งตัวพร้อมด้วยการ์ดที่สามารถต่อเข้ากับระบบบัสที่มีอีพรอมไว้สำหรับเก็บรายชื่อผู้ใช้และพาสส์เวิร์ด ผลิตภัณฑ์พวกนี้มักมีราคาถูกและสามารถให้การรักษาความปลอดภัยได้ในระดับที่ค่อนข้างดี เนื่องจากสามารถป้องกันไม่ให้ผู้ใช้ทำการบูตเอ็มเอสดอสจากฟลอปปี้ดิสค์ไดรฟ์หรือฮาร์ดไดรฟ์จนกว่าจะใส่พาสส์เวิร์ดที่ถูกต้องเข้าไป เช่น พีซีซีเคียวริตี้บอร์ดของบริษัทแบล็อคบ็อกซ์และเซอร์เกนต์-แอกเซสคอนโทรลการ์ดของบริษัทอินดรัสเตรียลคอมพิวเตอร์รีซอร์ส ที่ผลิตผลิตภัณฑ์ในด้านการแสดงตนออกจำหน่าย พีซีซีเคียวริตี้บอร์ดสามารถเก็บพาสส์เวิร์ดได้หนึ่งคำและจะทำหน้าที่ป้องกันด้วยพาสส์เวิร์ดก่อนที่คอมพิวเตอร์จะบูตเอ็มเอสดอส นอกจากนี้ผู้ใช้ยังสามารถเลือกว่าเมื่อใดจึงจะใช้หรือไม่ใช้คุณลักษณะเด่นของการรักษาความปลอดภัยข้อมูลที่มีอยู่บนบอร์ดได้ตามใจชอบ คุณลักษณะเด่นของระบบการรักษาความปลอดภัยข้อมูลอีกอันก็คือออดิตติ้งที่มีไว้คอยสอดส่องการพยายามเข้าไปใช้เครื่อง บอร์ดแบบนี้มีมาพร้อมดิสเกตต์หนึ่งแผ่นเพื่อใช้สำหรับเซตคอนฟิกกูเรชันของระบบ ส่วนเซอร์เกนต์แอกเซสคอนโทรลการ์ดก็จะมีพาสส์เวิร์ดโปรเทคชันสำหรับก่อนที่จะบูตดอส ผลิตภัณฑ์นี้จะอยู่ในรูปของการ์ดที่เก็บพาสส์เวิร์ดได้ 10 คำ อันทำให้ผู้ใช้หลาย ๆ รายสามารถใช้เวอร์กสเตชันเดียวกันได้ โดยแต่ละรายก็มีพาสส์เวิร์ดเป็นเฉพาะของตนเอง ซอฟต์แวร์ของกรณีนี้จะอยู่ในการ์ดตั้งแต่ต้นจึงไม่จำเป็นต้องใช้ดิสค์อินสตอลเลชัน



2. ผลิตภัณฑ์ทางด้านจำกัดการเข้าถึงข้อมูลทางไกล

แม้ว่าผู้บริหารระบบแลนจะไม่ต้องการให้ผู้ใช้ที่อยู่ไกลออกไปโทรเข้ามาหาแลนในบริษัทก็ตาม แต่ก็ห้ามความต้องการของผู้ใช้ประเภทนี้ที่นับแต่จะมากขึ้นเรื่อย ๆ ไม่ได้ เมื่อเป็นเช่นนี้การติดต่อโดยหมุนโทรศัพท์เพื่อเข้าสู่เน็ตเวอร์กจึงสร้างปัญหาได้มาก โดยเฉพาะปัญหาที่เกิดจากพวกมือบอนที่อยากรู้อยากเห็นที่เรียกว่า "แฮกเกอร์" ที่จะใช้พีซีส่วนตัวพร้อมด้วยโมเด็มไว้สำหรับชอนไชเข้าไปในเน็ตเวอร์กด้วยโทรศัพท์และเดาพาสส์เวิร์ดจนถูกต้องเสร็จแล้วก็จะจัดการคัดลอกหรือเปลี่ยนแปลงสิ่งที่อยู่ในไฟล์อย่างสนุกมือ วิธีแก้ปัญหาทำนองนี้โดยไม่ต้องลงทุนมากนั้นทำได้โดยอาศัยการติดตั้งโมเด็มชนิด dial-back หรือ "dumb" dial-back และดีไวซ์อื่น ๆ ตัวอย่างของผลิตภัณฑ์ตัวแรกที่อยู่ในกลุ่มนี้เป็นของบริษัทเซาต์อีสต์อิเล็กทรอนิกส์ที่ทำออกมาในรูปของ SM-21 Call Back 212A Security Modem ที่สามารถให้การสนับสนุนจำนวนผู้สามารถโทรติดต่อเข้ามาถึง 200 จำนวน กับพาสส์เวิร์ดชนิดผสมกันและสามารถกำหนดว่าจะใช้โมเด็มแบบ 1200 baud หรือไม่ใช้ก็ได้ รวมทั้งการมีคุณลักษณะด้านออดิตติ้งให้ด้วยเพื่อไว้สำหรับสอดส่องการพยายามที่จะ Login จากภายนอก ผลิตภัณฑ์สุดท้ายที่จะพูดในที่นี้จะเป็นของบริษัท

PC Security Board $159
Black Box Corp.
P.O. Box 12800
Pittsburgh, PA 15241
(412) 746-5530
Circle reader service number 250

Sergeant Access Control Card $419
Industrial Computer Source
P.O. Box 23058
San Diego, CA 92123
(800) 523-2320
Circle reader service number 251

SM-21 Call Back 212A Security Modem $495 and up
South Hills Electronics
760 Beechnut Dr.
Pittsburgh, PA 15205
(800) 245-6215
Circle reader service number 252

Security Access Controller II (SACII) $450 and up
Control Cable Inc.
7261 Ambassador Rd.
Baltimore, MD 21207
(301) 298-4411
Circle reader service number 253

ปที่ 4 ข้อมูลของผู้จำหน่ายผลิตภัณฑ์การรักษาความปลอดภัยในแลนที่เป็นรายย่อย

คอนโทรลเคเบิ้ล ในสหรัฐฯที่ผลิต SMarT-1 Security Access Controller II (SAC II) ในรูปของ Call-back ดีไวซ์ออกจำหน่ายโดยในขณะใช้งานจะต้องต่อเข้ากับตัวโมเด็มที่ติดอยู่กับคอมพิวเตอร์ SAC II มีหน่วยความจำขนาด 1000 ตัวเลข/พาสส์เวิร์ด และการเข้าถึงดีไวซ์ตัวนี้จะอยู่ในรูปของโปรแกรมที่จะขึ้นกับ "เวลา" ของแต่ละวัน ผู้เรียกเข้ามาที่ไม่ถือว่ามีสิทธิก็จะถูกตัดสายโดยอัตโนมัติ รวมทั้งการมีเส้นทางการตรวจสอบไว้ให้ผู้ใช้สามารถติดตามสั่งต่าง ๆ ได้ด้วย ระบบ SAC II นี้สามารถใช้งานได้โดยไม่ขึ้นกับความเร็วของโมเด็มและโปรโตคอลใด ๆ รวมทั้งไม่ขึ้นกับวิธีการในด้านเอ็นคริปชันอีกด้วย

สรุป

การรักษาความปลอดภัยในระบบเน็ตเวอร์กในยุคปัจจุบันได้ก้าวมาถึงขั้นของการมีผลิตภัณฑ์ต่างๆ โดยเฉพาะที่เกี่ยวกับการรักษาความปลอดภัยในระบบแลนที่สามารถสนองความต้องการผู้ใช้ที่เต็มไปด้วยความซับซ้อนของหน่วยงานใหญ่ ๆ เช่นกระทรวงกลาโหมสหรัฐฯ ได้เป็นอย่างดี อันเป็นนิมิตหมายว่าภาคเอกชนก็จะมีสิทธิได้ใช้ผลิตภัณฑ์คุณภาพสูงเช่นนี้ในไม่ช้า